Department of Homeland Security Daily Open Source Infrastructure Report for 06 February 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Palm Beach Post reports a carbon monoxide build−up, caused by a roof tarp that covered a boiler vent, sickened more than a dozen people and forced the evacuation of 300 from the YMCA of Boca Raton, Florida. (See item 7)
- The Associated Press reports a series of fires erupted in isolated churches along rural back roads south of Birmingham, Alabama, destroying or damaging five houses of worship in what authorities called an arson case with no discernible motive. (See item 42)
- The San Antonio News reports that improvised explosive devices −− the home made bombs which have killed and maimed so many U.S. troops in Iraq −− were seized along with automatic weapons, grenades, gunpowder, and ammunition in raids in the Texas border city of Laredo. (See item 43)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 03, Rutland Herald (VT)* — **Vermont says Yankee emergency drill problems fixed.** The state says it has resolved all but a few of the "miscellaneous" problems from last spring's emergency preparedness drill for the emergency zone around the Vermont Yankee

nuclear power plant. Last summer, the Federal Emergency Management Agency (FEMA) gave the state Emergency Management Office marks so low that parts of the drill had to be replayed and re−evaluated within 120 days. The federal agency said that in the event of a real emergency, the public would have unnecessarily been exposed to additional radiation, and that false, confusing and misleading information had been released to the public by a disorganized state office. In a real emergency, FEMA noted, the problems could have "caused mass confusion." FEMA concluded about the plume−exposure pathway drill on May 25−26: "The state of Vermont failed to provide adequate direction and control over the public alert and notification system." The final report, which recently was released to the public, identified seven "deficiencies" and 25 areas needing corrective action. The problems ranged from delayed evacuations, delayed notice to the public, lack of critical information necessary to evacuate, and lack of communication equipment to keep emergency workers in touch with federal and state authorities.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20060203/NEWS/602030364/1003

2. *February 03, Associated Press* — **Guns used to guard California nuclear laboratory.** Officials at the Lawrence Livermore National Laboratory have added a new weapon to their armory: a high−powered machine gun that can fire more than 50 rounds a second. The weapon, unveiled Thursday, February 2, is a six−barrel Gatling gun called the Dillon Aero M134D. An undisclosed number of the guns will be mounted on vehicles and elsewhere at the lab. "What we want to do is equip our protective force with the capability that will leave no doubt about the outcome," said Linton Brooks, head of the National Nuclear Security Administration. Lab spokesperson Susan Houghton said the guns add "one more layer of protection." The 8,000−employee lab is 50 miles east of San Francisco, CA.
Source: http://www.guardian.co.uk/worldlatest/story/0,,−5590184,00.h tml

3. *February 02, Chicago Tribune (IL)* — **Nuclear industry planning new reactors.** No nuclear plants have been licensed since 1978, but utility companies nationwide are considering building at least 10 new reactors, according to the Nuclear Energy Commission. Last year at this time, only three new reactors were under consideration. Any new plant is years away, although one utility says it hopes to begin construction in four years. Scott Burnell, spokesperson for the NRC, said the reason for the proposed building was "...passage of the energy policy act last year...Utilities started getting into detailed discussions with us." Marilyn Kray, president of NuStart Energy Development LLC, a consortium of utilities, said, "The investment incentives in [last year's] energy bill will help offset some of the risks" of building a new nuclear plant. NuStart is trying to obtain two licenses for new nuclear plants, possibly to be built in Scottsdale, AL, and near Port Gibson, MS. Chairman John Rowe says Exelon is not enthusiastic about building a new plant unless the government approves a final disposal plan for spent nuclear fuel. Entergy has plans to add reactors to existing plants at Port Gibson and St. Francisville, near Baton Rouge, LA. Construction of the Port Gibson reactor is scheduled for 2010.
Source: http://www.chicagotribune.com/business/chi−0602020168feb02,1,4004259.story?track=rss

4. *February 02, Associated Press* — **Columbia Gas Transmission plans to expand gas pipeline, storage networks.** NiSource Inc. on Thursday, February 2, said subsidiary Columbia

Gas Transmission plans to expand its pipeline, compression, and storage networks to boost gas supply to four distribution companies in Virginia and Pennsylvania. The expansion is expected to increase supply by 97,050 dekatherms per day when it begins operation, which is scheduled for April 2009. Four gas utilities have arranged 15−year agreements for the storage and transportation services.
Source: http://biz.yahoo.com/ap/060202/nisource_pipeline_expansion.h tml?.v=1

5. *February 02, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission issues letter on electric grid reliability.** The Nuclear Regulatory Commission (NRC) staff has issued a generic letter asking all U.S. nuclear power plant operators for additional information on how they continue to ensure the reliability of offsite electrical power sources and how they continue to comply with NRC regulations on maintaining offsite power to safety−related systems. When the grid is lost or significantly degraded, the protective circuits of the nuclear reactor and the turbine generator automatically shut down the plant. Nuclear facilities are designed with backup power sources to provide power to essential safety systems. The NRC's review of the events surrounding the August 2003 blackout raised several issues, including how plants prearrange for backup power from local sources. Plant operators have 60 days from the issuance of the Letter to submit written responses to questions in several areas, including: arrangements between the plants and grid system operators or reliability coordinators, to monitor the grid's ability to provide power to a plant's safety systems; arrangements for system operators to assist plants in considering grid conditions for assessing risks related to performing grid−risk sensitive maintenance; and, procedures for identifying local power sources that could assist the plant when normal offsite power is unavailable.
Letter: http://www.nrc.gov/reading−rm/doc−collections/gen−comm/gen−l etters/2006/index.html.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 13.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *February 04, KITV−TV (HI)* — **Chemical odor prompts building evacuation in Hawaii.** Part of the American Savings Bank building in downtown Honolulu, HI, was evacuated on Friday, February 3, because of a suspicious chemical odor. An employee in the building noticed an unusual smell and reported it to the Honolulu Fire Department (HFD). The evacuation happened at about 3 p.m. local time. Only occupants of the 14th floor and above were asked to evacuate, HFD officials said. People waited outside for about an hour before they were able to return to the building. The bad smell remains a mystery. The fire department was not able to determine what it was or where it was coming from.
Source: http://www.msnbc.msn.com/id/11168652/from/RSS/

7. *February 04, Palm Beach Post (FL)* — **YMCA evacuated due to carbon monoxide in Florida.** A carbon monoxide build−up sickened more than a dozen people and forced the evacuation of 300 from the YMCA of Boca Raton, FL, Saturday morning, February 4. At least 13 people went to area hospitals after falling ill with headaches, dizziness and nausea shortly before 10 a.m. EST. The cause of the incident appeared to be a roof tarp that covered a boiler vent, a Palm Beach County Fire Rescue official said. Fire Rescue officials recorded levels of

carbon monoxide up to 10 times higher than what is considered safe. The highest levels were near the ceiling and not in populated areas of the YMCA, Fire Rescue District Chief Billy Schmidt said. But 40 to 50 people were in affected parts of the building, which houses the swimming pool, locker rooms and fitness center. Another 250 people were evacuated from elsewhere in the building, as a precaution. Effects of carbon monoxide poisoning can range from dizziness, headaches and nausea to organ damage and death. The building was cleared of carbon monoxide by early afternoon and will reopen Monday, February 6, a YMCA spokesperson said.
Source: http://www.palmbeachpost.com/localnews/content/local_news/epaper/2006/02/04/0204evacuate.html

8. *February 03, Associated Press* — **Chemical spill in California prompts interstate closure.** An overturned tractor−trailer leaked a caustic chemical onto Highway 152 in Mercer County, CA, on Friday morning, February 3. The trailer was loaded with more than a dozen containers of hydroxylamine sulfate when it rolled onto its side around 8 a.m. PST in the eastbound lane near the intersection with Interstate 5 in Merced County, according to the California Highway Patrol (CHP). The driver suffered minor injuries. The accident shut down traffic in all directions of Highway 152 and I−5 at the intersection, as a hazardous material cleanup crew worked to clean up the chemical, which is used in the manufacture of textiles, paints, varnishes, rust−proofing, synthetic rubber and other chemicals. It was not clear how much of the chemical leaked onto the highway, said CHP Officer Mark McWilliams.
Source: http://www.mercedsunstar.com/state_wire/story/11768000p−1248 7804c.html

9. *February 03, WSYR−TV (NY)* — **Forty−three sick from carbon monoxide fumes at New York hair institute.** Several ambulances and fire crews were sent to the Phillips Hair Styling Institute at 709 East Genesee Street in Syracuse, NY, Friday morning, February 3, because 43 people were overcome by carbon monoxide fumes. Twenty−nine victims were sent to Syracuse University Hospital. Twenty−eight of them have been released. Doctors are checking one patient, because the patient has an existing condition that may have been affected by the carbon monoxide. Five victims were taken to Crouse Hospital, five more patients were treated at St. Joseph's and four were treated and released from Community General Hospital. National Grid says the carbon monoxide leak was most likely caused by a furnace or hot water heater in the basement of the building. The equipment cannot be used until repairs are made, and National Grid makes another inspection.
Source: http://www.9wsyr.com/news/local/story.aspx?content_id=78455B5E−538D−4DF2−9C87−CC6159101FFE

[Return to top]

Defense Industrial Base Sector

10. *February 03, U.S. Department of Defense* — **Report of the 2006 Quadrennial Defense Review released.** The Report of the 2006 Quadrennial Defense Review (QDR) was released Friday, February 3. Within the document, the Department of Defense's (DoD) senior leadership sets out where the DoD currently is and the direction they believe it needs to go in fulfilling their responsibilities to the American people. The 2006 Quadrennial Defense Review reflects a process of change that has gathered momentum since the release of its predecessor QDR in

2001. The ideas and proposals in this document are provided as a roadmap for change. The QDR is not a programmatic or budget document. Instead, it reflects the thinking of the senior civilian and military leaders of the DoD: 1) Need to “find, fix and finish” combat operations against new and elusive foes; 2) Need for considerably better fusion of intelligence and operations to produce action plans that can be executed in real time; 3) Realization that everything done in DoD must contribute to joint war−fighting capability; 4) Central reality that success depends on the dedication, professionalism and skills of the men and women in uniform.
Source: http://www.defenselink.mil/qdr/report/Report.pdf

[Return to top]

Banking and Finance Sector

11. *February 03, Finextra* — **Russian Trading System Stock Exchange disrupted by virus attack.** A computer virus attack caused the Russian Trading System (RTS) Stock Exchange to suspend trading on its three main markets Thursday, February, 2. The malware infected an Internet−connected computer and generated a large amount of outgoing e−mail traffic. Legitimate incoming and out going email was interrupted by the virus's activities. Trading was suspended for over an hour on Thursday afternoon while the Exchange tracked down the source of the outbreak. RTS vice president Dmitry Shatsky said, "The virus got into a computer connected to a test trading system from the Internet...The infected computer started generating huge volumes of parasitic traffic, which overloaded the RTS's support routers. The result was that normal traffic −− data going into and out of the trading system −− was not processed." Graham Cluley, Sophos technology consultant says the attack should act as a wake−up call for any business not taking the virus threat seriously. "While all the world was in a frenzy over the Nyxem damp squib, this attack infiltrated the RTS and could have potentially given hackers access to their systems," he says. Trading has resumed at the Exchange, which claims that no data was stolen during the assault.
Source: http://finextra.com/fullstory.asp?id=14867

12. *February 03, Lincoln County News (ME)* — **E−mail scam targets Maine bank customers.** Customers of The First National Bank of Damariscotta, ME, have received a series of fraudulent communications: e−mails inviting them to submit personal account information through a link that mimicked the appearance of the First National’s Website. First National president and CEO Dan Daigneault confirmed the e−mails are not connected to the bank. Daigneault stressed that all information First National customers have legitimately supplied the bank remains secure. The discredited e−mails read in part: "The First Bank has a strict policy to ensure all of our customer’s emails associated with their bank account(s) are confirmed. Upon inspection this email was registered with your account(s), however not confirmed. Please confirm your email by clicking the link below:..." The link brings up what appears to be a legitimate web page connected to The First National Bank. Respondents are asked to log in with their account information and personal identification numbers. The e−mail threatens that failure to comply will result in the suspension of online banking privileges. Daigneault said that bank employees first became aware of the ongoing scam late Sunday, January 29. In subsequent e−mails, the recipient is asked to click on a link which includes the partial address "http:cash4erotik.de…"

Source: http://www.mainelincolncountynews.com/index.cfm?ID=16766

13. *February 02, Vnunet* — **Britain reconfigures identity theft fraud costs, higher than previously thought.** The Home Office has upped its estimates of the cost to the UK of identity fraud. The new study included costs to the telecom industry which had been left out of the original statistics. "The very nature of the services provided by the telecom industry makes us a target for identity fraud," said Jack Wraith, chief executive at the Telecommunications UK Fraud Forum. Home Office minister Andy Burnham has been quick to suggest that a national identity card scheme, such as a currently introduced bill, would solve the problem. "One way we can reduce the potential for identity fraud is to introduce a national identity card, backed by a National Identity Register, using biometric technology to crack down on multiple identities and secure personal data on behalf of the individual." But in an interview last year the then head of the National High tech Crime Unit said identity cards would do little to cut identity fraud, suggesting instead that they would simply spawn a market in fakes. David Hill, security consultant at Red 24, said "Simple measures like shredding documents that contain any personal information can significantly reduce the risk of your identity being assumed by someone else."
Source: http://www.vnunet.com/vnunet/news/2149676/home−office−ups−id entity−fraud

[Return to top]

Transportation and Border Security Sector

14. *February 04, CNN* — **Officials: Fire made ferry sink.** Egypt's transport minister said a blaze aboard an Egyptian ferry set off a sequence of events that led it to sink Friday, February 3, in the Red Sea, causing what officials fear may be around 1,000 deaths. The minister said Saturday, February 4, an initial investigation showed a truck erupted in flames in the hold of the ship. After the crew tried to put out the fire, the captain's efforts to turn the boat around caused it to tilt in heavy winds and ultimately sink. The seas were rough when the Al Salam Boccaccio 98 capsized, said Transport Minister Mohamed Loutfy Mansour. State−run Nile Television said Saturday there were 389 survivors. By daylight Saturday, 185 bodies had been pulled from the 3,000−foot−deep waters, officials said. A Maritime Transport spokesperson said the Al Salam Boccaccio 98 was certified to carry passengers until 2010 and was fully compliant with maintenance regulations. However, one man in the crowd told CNN he had taken the same ship on the same route a month ago and that the ship appeared overloaded on that trip, packed with passengers and laden with eight large trucks filled with freight, the man said. He also said the clasps that secured lifeboats to the ship were rusted.
Source: http://www.cnn.com/2006/WORLD/meast/02/04/egypt.ship/index.h tml

15. *February 03, USA TODAY* — **British fuel rationing threatens U.S.−London flights.** U.S. airlines are chafing under the added costs of a jet fuel shortage at London Heathrow airport, and travelers to Great Britain may face fewer flight options as a result. James May, head of the U.S. airline trade group Air Transport Association, said Thursday, February 2, that No. 2 United Airlines has delayed introduction of a second daily flight from Los Angeles to Heathrow because of fuel issues. A December 11 explosion and fire at Buncefield, one of Britain's biggest fuel depots, has reduced jet fuel supplies to Heathrow. Buncefield normally supplies 30 percent of the fuel sold at Heathrow, the world's busiest international airport. In response to the supply

disruption, privately held airport operator BAA imposed rationing rules that U.S. carriers and the U.S. government call unfair. The rationing program allows British airlines 82 percent of their normal jet fuel allocation on flights longer than five hours, versus 70 percent for non−UK airlines. American and United are making up for the limitation by hauling extra fuel when they fly to Heathrow. Because the planes must burn 20 percent more fuel just to carry the weight of the fuller tanks, that greatly cuts into potential profits on their trans−Atlantic routes.
Source: http://www.usatoday.com/travel/flights/2006−02−02−london−fue l−usat_x.htm

16. *February 03, Associated Press* — **Northwest wants to hire non−U.S. flight attendants for international flights.** Northwest Airlines wants to replace 30 percent of its flight attendants on international flights with non−U.S. flight attendants, roughly 800 people, to cut costs so that it can emerge from bankruptcy, a company executive testified in a New York bankruptcy court Thursday, February 2. Northwest, which filed for Chapter 11 bankruptcy protection in September, seeks to save $1.4 billion in wage and benefit costs. Thursday was the seventh day of hearings devoted to the airline's request to toss out collective bargaining agreements with the unions. Michael Becker, Northwest's senior vice president of human resources and labor relations, also testified that the foreign flight attendants would not be part of the U.S.−based flight attendants union, the Professional Flight Attendants Association. Becker said Northwest would save $20.2 million by hiring non−U.S. flight attendants. The carrier had maintained that it needed to hire foreign workers as flight attendants because of their language and culture skills to better serve international flights such as one between Narita, Japan, and Honolulu where 90 to 95 percent of its passengers are Japanese nationals.
Source: http://www.usatoday.com/travel/flights/2006−02−02−nwa−attend ants_x.htm

17. *February 03, Associated Press* — **Rushed repair job caused plane crash, board finds.** A mechanic rushed a repair job on a single−engine plane causing it to crash on a busy freeway, federal transportation safety officials said. The National Transportation Safety board ruled Wednesday, February 1, that mechanic Robert Lee Barber used improper parts to repair a broken exhaust valve on the Piper Turbo Arrow plane, failed to check whether pieces of the damaged valve had fallen into the engine, and spent just three hours to complete a job that he was told would take about 20 hours. The board concluded that the plane, which landed on Interstate 680 shortly after takeoff on April 13, 2004, crashed because of a loss of engine power due to improper maintenance repair procedures and use of improper parts. The pilot, Robert Curt Hatch, and his son were unhurt in the crash.
Source: http://www.insidebayarea.com/trivalleyherald/localnews/ci_34 71742

18. *February 03, Mobile Register (AL)* — **Weapon slipped airport's security.** A man traveling to Ohio last year passed through airport security in Mobile, AL, with a loaded handgun, according to the FBI. Nevertheless, federal authorities in charge of screening passengers at Mobile Regional Airport said they believe air travel remains safe at the terminal, which has been held up as a model for security upgrades at similarly sized airports throughout the country. The gun was not discovered until the passenger, William M. Owens of Mobile, tried to board a return flight in Columbus, OH, on May 4. Airport screeners spotted the .38−caliber snub−nosed revolver with an X−ray machine and alerted law enforcement authorities, according to an affidavit filed by the FBI. Owens, 63, pleaded guilty Wednesday, February 1, in U.S. District Court in Mobile to a misdemeanor offense of entering an aircraft or airport area in violation of security. Lauren Stover, a spokesperson for the Transportation Security Administration, said

that shortly after the incident authorities reviewed videotapes and questioned screeners on duty at the time Owens passed through. She said the investigation was inconclusive about whether the revolver was inside his black leather shoulder bag.
Source: http://www.al.com/news/mobileregister/index.ssf?/base/news/1138961877182540.xml&coll=3

[Return to top]

Postal and Shipping Sector

19. *February 05, Associated Press* — **Man charged with sending hoax letters, including to President Bush.** A man accused of mailing hundreds of anthrax hoax letters −− including one to President Bush −− was arrested Friday, February 3, two days after he was charged with threatening the use of a weapon of mass destruction. Derek Brodie, 42, of Asbury Park, NJ, sent more than 200 of the letters, each containing a white sheet of paper with the word "anthrax" written vertically in multi−colored block letters, according to the FBI. The letters, which contained no return addresses, were sent to government agencies, media personalities, actors and actresses and businesses. He had a habit of using the same rainbow−colored pencil," said FBI Special Agent Steve Siegel. "He was sending these out to hundreds of people, various governmental agencies, media people, actresses." None of the envelopes contained anthrax, the biological agent used in a series of unsolved 2001 mailings that killed five people. All were tested at a New Jersey Department of Health and Senior Services laboratory, Siegel said. The mailings apparently began in May 2005. Twenty of the letters were intercepted by U.S. Postal Service employees in Freehold Township and Westfield in May and June, according to a complaint filed by Special Agent David Goldkopf. Brodie is being held without bail pending a psychiatric evaluation.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−anthraxhoax−lette0203feb03,0,748607.story?coll=ny−region−apne wjersey

[Return to top]

Agriculture Sector

20. *February 03, Agricultural Research Service* — **Sources of sorghum anthracnose resistance discovered.** Agricultural Research Service (ARS) scientists scouring sorghum germplasm collections from African countries in search of anthracnose resistance for this grain crop were surprised to find some key sources in unexpected locales. Since pathogens can overcome plant resistance, researchers need to find new sources of resistant germplasm that breeders can use. ARS research geneticist John Erpelding looked to sorghum collections from African countries for resistance to the anthracnose pathogen. The fungus infects all aboveground parts of the plant and, in severe cases, the disease can kill plants before maturity. Often, anthracnose weakens the plant, severely reducing grain yield and quality. Erpelding was not surprised to find resistance in about half of the lines evaluated from a subset of the Sudan collection, considered a center of diversity for sorghum. But finding 80 percent of the accessions from a subset of the Mali collection to be resistant was unexpected. So, the researchers evaluated additional germplasm subsets representing specific regions of Mali and found an association between weather pattern

and anthracnose resistance. More accessions from dry areas were susceptible, while nearly all from the wettest region were resistant. The U.S. produces about one−fifth of the world's sorghum and is the leading exporter of grain sorghum.
Source: http://www.ars.usda.gov/is/pr/2006/060203.htm

21. *February 03, Monterey Herald (CA)* — **Protecting crops a top priority.** Preparing and protecting the California agricultural industry from potential pest invasions, diseases, and bioterrorist attacks will be a top priority this year, California Department of Food and Agriculture Secretary A.G. Kawamura said Thursday, February 2. The governor's proposed budget for agricultural programs for the 2006−07 fiscal year, outlined in a handout Monterey, CA, meeting participants received, lists eight million dollars of the $285 million proposed for the state's Department of Food and Agriculture this year as focused on infrastructure−specific programs. About seven million dollars would go towards emerging threats programs which include those which protect the industry against plant and animal disease outbreaks, provide community outreach to educate people about the risks and techniques to prevent disease, and the expansion of laboratory capacity for rapid testing. "Our programs generally have emergency response components to them," said Steve Lyle, spokesperson for the State Department of Agriculture. But they have never been pulled out and funded separately, he said, and this will "improve our capacity to respond to agricultural emergencies beyond our current capacity," he said.
Source: http://www.montereyherald.com/mld/montereyherald/13782790.ht m

22. *February 03, Dow Jones Newswires* — **U.S. animal movement database rolled out.** The National Animal Movement Database, which will allow U.S. Department of Agriculture (USDA) officials to trace an animal or group of animals back to their source, was rolled out Thursday, February 2. The system was explained by members of its board of directors to a gathering of cattle producers at the annual National Cattlemen's Beef Association convention in Denver, CO. In an interview with reporters after the presentation, database directors confirmed that the system is designed to be a single database for the nation. Charles Miller, chairman of the directing organization called the U.S. Animal Identification Organization, said the system seeks and stores only four pieces of data: the premises identification number, the individual animal or the group number, the date of the "event" necessitating the input of information into the Web−based system and the "event" code, which identifies whether the event is the birth, first sale, slaughter or a list of other possibilities. The board members said the system currently is being tested, but an announcement about when producers can begin inputting data is expected within a few weeks.
Source: http://www.agriculture.com/ag/futuresource/FutureSourceStory Index.jhtml?storyId=41700199

[Return to top]

Food Sector

23. *February 02, Food Production Daily* — **Handheld sensor detects pathogens within minutes.** A handheld sensor could help food companies quickly detect within 10 minutes whether their products are laden with E. coli or listeria −− before they are shipped out of the plant. Raj Mutharasan, an engineer at Drexel University, has developed the technology. Detecting the bug

in plants is a slow process that involves removing whole batches of foodstuffs from production lines while cultures are grown or DNA amplified. The device works by detecting how the mass of a few E coli cells changes the vibration of a miniature glass beam. The sensor is made up of a sliver of glass. The glass is fixed at one end and has a layer of piezoelectric ceramic called lead zirconate titanate (PZT) glued to the other. The glass sliver is coated with antibodies to E. coli 0157:H7, the strain that causes foodborne illness. An alternating voltage applied to the piezoelectric layer makes it expand and contract, causing the sliver to vibrate. The vibration is greatest at the sliver's resonant frequency. Changes in the resonant frequency as E. coli cells bind to the antibodies provide a measure of the concentration of the pathogen.
Source: http://www.foodproductiondaily−usa.com/news/ng.asp?n=65558−sensor−pathogen−e−coli

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

24. *February 04, Reuters* — **Indonesia says four more bird flu cases confirmed.** A Hong Kong laboratory recognized by the World Health Organization (WHO) has confirmed four more human bird flu cases in Indonesia, including two deaths, a senior Indonesian Health Ministry official said on Saturday, February 4. Hariadi Wibisono, the ministry's director of control of animal−borne diseases, said that raised Indonesia's total confirmed human bird flu cases to 23. "There are now 23 confirmed cases in Indonesia. Of these, 16 have died," Wibisono said. While it mostly affects birds, the H5N1 strain of bird flu has infected 161 people and killed 86 of them since 2003, according to WHO. Wibisono said the newly confirmed Indonesian deaths were of a 22−year−old male chicken seller from Jakarta who died late last month and a 15−year−old boy who died in the West Java city of Bandung this week.
Source: http://www.alertnet.org/thenews/newsdesk/L0489005.htm

25. *February 04, Richmond Times Dispatch* — **Ricin reported in home.** Chesterfield, VA, police say the discovery of the toxin ricin in a home is related to a domestic dispute. Ricin was found January 20 in the home of Chetanand Kumar Sewraz, police said Friday, February 3. Ricin, which has potential to be used as an agent of biological warfare, is widely available, easily produced and derived from the beans of the castor plant. Chesterfield police spokesperson Ann Reid said the ricin found was in a semi−solid mash form and poses no threat to the public.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1137833883217

26. *February 03, Agence France−Presse* — **Crippling mosquito−borne disease spreads to Mauritius.** At least two people have been diagnosed with a incurable, crippling mosquito−borne disease on Mauritius as the viral infection spread to a fourth Indian Ocean island, officials said. After health authorities on Madagascar, the Seychelles, and the French

overseas territory of Reunion reported outbreaks and boosted anti−mosquito campaigns, Mauritius, along with the Comoros, followed suit. "A nation−wide campaign to eradicate mosquitoes has been launched on the island," the government said in a statement detailing its efforts to halt the spread of chikungunya. The statement did not say if or how many people had been affected but a health ministry official, said there were two confirmed and 15 suspected cases since the beginning of the year. In the Comoros archipelago, where no cases have yet been reported, health officials said they were stepping up surveillance to guard against an outbreak. The worst hit island is Reunion, where doctors said Thursday, February 2, that 45,000 new cases of chikungunya had been reported since mid−December. On the Seychelles, nearly 2,000 people have been infected with the disease since November, officials said. Madagascar said dozens of people have flocked to a hospital in the country's second largest town of Toamasina, showing symptoms of the disease.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://news.yahoo.com/s/afp/20060203/hl_afp/healthindianocean_060203184917;_ylt=ArHV1TqYw6aY3JRYgyWzZaiJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

27. *February 03, U.S. Food and Drug Administration* — **Laboratory test to detect human infections with avian influenza A/H5 viruses approved.** The U.S. Food and Drug Administration (FDA) Friday, February 3, announced the approval of a new laboratory test to diagnose H5 strains of influenza in patients suspected to be infected with the virus. The test was developed by the U.S. Centers for Disease Control and Prevention (CDC). The test provides preliminary results on suspected H5 influenza samples within four hours once a sample arrives at the lab and testing begins. Previous testing technology would require at least two to three days to render results. If the presence of the H5 strain is identified, then further testing is conducted to identify the specific H5 subtype (e.g., H5N1). This test will be distributed to Laboratory Response Network (LRN)−designated laboratories to enhance early detection and surveillance activities as well as increase laboratory response capacity associated with a potential pandemic. Domestically the LRN is a system of about 140 labs in all 50 states. LRN labs have special experience and training in molecular testing methods, special bio−safety facilities and containment procedures as well as communication networks connected to public health programs across the country. CDC has also shared the test technology with the World Health Organization and its collaborating centers around the world.
Source: http://www.hhs.gov/news/press/2006pres/20060203.html

28. *February 03, U.S. Food and Drug Administration* — **U.S. Food and Drug Administration orders firm to stop tissue recovery.** The U.S. Food and Drug Administration (FDA) Friday, February 3, ordered Biomedical Tissue Services, Ltd. (BTS), of Fort Lee, NJ, a human tissue−recovery firm, to immediately cease all manufacturing operations. All tissue products initially recovered from human donors by BTS were recalled. FDA is carefully monitoring these recalls to account for all of the tissue distributed. "FDA's investigation of BTS revealed serious and widespread deficiencies in their manufacturing practices that provide the agency reason to believe that allowing the firm to manufacture would present a danger to public health by increasing the risk of communicable disease transmission," said Margaret Glavin, FDA's Associate Commissioner for Regulatory Affairs. The FDA order requires BTS to suspend any and all manufacturing steps, including but not limited to the recovery and shipment of tissue. FDA's inspection of BTS uncovered serious violations of the regulations governing donor

screening and record keeping practices, as well as failures to follow their own standard operating procedures, failure to recover tissue in a manner that does not cause contamination or cross−contamination during recovery, and failure to adequately control environmental conditions. Despite records maintaining otherwise, the firm had inadequately screened donors for risk factors for, or clinical evidence of, relevant communicable disease agents and diseases.
Source: http://www.fda.gov/bbs/topics/news/2006/NEW01309.html

29. *February 02, Journal of the American Medical Association* — **Adamantane resistance among influenza A viruses isolated early during the 2005−2006 influenza season.** The adamantanes, amantadine and rimantadine, have been used as first−choice antiviral drugs against community outbreaks of influenza A viruses for many years. Rates of viruses resistant to these drugs have been increasing globally. Researchers investigated the frequency of adamantane−resistant influenza A viruses circulating in the U.S. during the initial months of the 2005−2006 influenza season. Influenza isolates collected from 26 states from October 1 through December 31, 2005, and submitted to the U.S. Centers for Disease Control and Prevention were tested for drug resistance as part of ongoing surveillance. Isolates were submitted from World Health Organization collaborating laboratories and National Respiratory and Enteric Virus Surveillance System laboratories. Researchers identified viruses containing mutations within the M2 gene that are known to confer resistance to both amantadine and rimantadine. A total of 209 influenza A(H3N2) viruses isolated from patients in 26 states were screened, of which 92.3 percent contained a change at amino acid 31 in the M2 gene known to be correlated with adamantane resistance. Two of eight influenza A(H1N1) viruses contained the same mutation. The high proportion of influenza A viruses currently circulating in the U.S. demonstrating adamantane resistance highlights the clinical importance of rapid surveillance for antiviral resistance.
Source: http://jama.ama−assn.org/cgi/content/full/295.8.joc60020v1

30. *February 02, Agence France−Presse* — **Russia allocates millions to combat bird flu.** Russia has allocated more than US$43 million to combat bird flu, Health Minister Mikhail Zurabov said, as Moscow braced for fresh cases of the disease with the start of bird migrations. Some $12 million would be spent on identifying cases of bird flu and diagnosing the disease in Russia and elsewhere in the Commonwealth of Independent States (CIS), a grouping of former Soviet republics excluding the Baltic states, the minister said. No cases of the H5N1 strain of the bird flu virus have been found in humans in Russia but the disease has been detected in fowl since the middle of last year and hundreds of thousands of birds have been culled.
Source: http://news.yahoo.com/s/afp/20060202/hl_afp/healthflurussia_060202184344;_ylt=AuFfQ.t4OpVPg78JrvsPi7WJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *February 06, San Francisco Examiner (CA)* — **California officials to study earthquake response.** About 75 officials from throughout San Francisco, CA, will be traveling on the tab of the Federal Emergency Management Agency (FEMA) this March to fine−tune their earthquake response plans at an emergency conference in Maryland. Dozens of city and county staff will join representatives from local hospitals, school districts and San Francisco International Airport from March 6 to March 10 in Emmitsburg, MD, for an emergency management course at FEMA's National Emergency Training Center. The training comes as officials gear up for an April 20 countywide disaster exercise, the area's first since 2004. The course will focus on earthquake preparedness and was specifically designed to help the county test its emergency response plans, said Supervisor Bill O'Callahan of the San Mateo County Sheriff's Office of Emergency Services. Participants will be divided into five sections −− command, operations, planning, logistics and finance −− according to a protocol laid out by the Standardized Emergency Management System, O'Callahan said.
Source: http://www.sfexaminer.com/articles/2006/02/02/peninsula/2006 0202_pe03_quake.txt

32. *February 02, News Horn (LA)* — **Louisiana governor establishes panel to direct creation of statewide system for first responders.** Created through Executive Order to address the need for compatible and effective communication among first responders, Louisiana Governor Kathleen Babineaux Blanco has charged the Statewide Interoperable Communication System Executive Committee to develop a statewide, user−driven approach among all levels of government to provide reliable communications for the entire emergency response community. The committee, which will consist of communications and first responder experts, is charged with immediately addressing communications challenges experienced by emergency personnel in the aftermath of Hurricanes Katrina and Rita. The committee will work in concert with efforts already underway to improve interoperability in Louisiana. Since September 11, Louisiana has been making efforts to improve its communication systems. "Communication is critical to direct emergency response. Emergency responders must be able to talk to one another. You can't coordinate if you can't communicate," said Governor Blanco. "What we experienced in Katrina was not a failure to communicate, but an inability to communicate." The committee, as established in Executive Order No. KBB 2006−4, is charged with several duties, including designing, constructing, administering, and maintaining a statewide shared voice, data, and imagery communication system.
For more information on Louisiana's efforts: http://www.lsp.org/index.html
Full text of Executive Order No. KBB 2006−4:
http://www.gov.state.la.us/assets/docs/Executive_Orders/4exe cInteroperableCommunicationSystem.pdf
Source: http://www.newshorn.com/index.php?option=com_content&task=vi ew&id=799&Itemid=120

33. *February 02, National Oceanic and Atmospheric Administration* — **National severe weather workshop to be held in March.** Emergency managers and members of the media will have an opportunity to exchange information and techniques for public safety during severe weather, with academia and federal government experts from the National Oceanic and Atmospheric Administration (NOAA) at the sixth annual National Severe Weather Workshop on March 2−4, 2006, in Midwest City, OK. Registration is underway for the three−day workshop, which is

designed to enhance partnerships between severe weather forecasters and researchers, emergency managers, broadcast meteorologists, businesses, storm spotters and other weather enthusiasts. "This annual event brings together the people who are on the front lines when our country faces severe and hazardous weather situations," said retired Brig. Gen. David L. Johnson, director of the NOAA National Weather Service. A new activity this year will be a role−playing scenario with three teams representing the NOAA National Weather Service, broadcast meteorologists and emergency managers. The teams will simulate real−life situations in an actual weather event and explore information needs for decision making by those involved in real−time warning operations and information dissemination.
NOAA National Severe Weather Workshop 2006: http://www.norman.noaa.gov/nsww2006/
Source: http://www.noaanews.noaa.gov/stories2006/s2571.htm

[Return to top]

Information Technology and Telecommunications Sector

34. *February 03, Christian Science Monitor* — **Internet jihad: Tackling terror on the Web.** Nearly 18 months ago, Babar Ahmad, a British citizen, was arrested on an extradition request to the U.S. Charged with running Websites hosted in the U.S. that promoted and supported Islamic militancy, Ahmad remains in British custody. He has appealed the extradition order and Britain's High Court will hear the case on Monday, February 20. The proceedings will test the ability of Western governments to put on trial Islamic radicals who use the Internet as a key recruiting and organizational tool. But while the U.S. government pursues those who operate Websites that allegedly encourage terrorism, some argue that the authorities should instead concentrate on shutting down the sites themselves as soon as possible to limit their impact. Ahmad's case illustrates how seriously the U.S. is taking such Websites. His extradition warrant accuses him −− among other things −− of helping to run azzam.com, one of the earliest and most high profile English−language pro−jihad Websites, which for a time was run by an Internet Service Provider (ISP) headquartered in Connecticut. A federal grand jury in the U.S. indicted Ahmad in October 2004 on four charges. If found guilty, he faces life imprisonment.
Source: http://www.csmonitor.com/2006/0203/p06s02−woeu.html

35. *February 02, FrSIRT* — **Mozilla products have multiple memory corruption and security bypass issues.** Multiple vulnerabilities were identified in Mozilla Suite, Mozilla Firefox and Thunderbird, which may be exploited by remote attackers to take complete control of an affected system or bypass security restrictions. The first issue is due to errors in the JavaScript engine that fails to properly protect certain temporary variables during garbage collection. The second flaw is due to a memory corruption error when dynamically changing the style of an element from "position:relative" to "position:static." The third vulnerability is due to an error when handling large history information passed in the "history.dat" file. The fourth issue is due to a memory corruption error when calling the "QueryInterface" method of the built−in Location and Navigator objects. The fifth flaw is due to an error in the "XULDocument.persist()" function that does not properly validate the attribute name. The sixth vulnerability is due to integer overflow errors in the E4X, SVG, and Canvas features. The seventh issue is due to an error in the XML parser. And the eighth flaw is due to an error in the E4X implementation that exposes the internal "AnyName" object to Web content.
Solution: Upgrade to Firefox 1.5.0.1 or SeaMonkey 1.0: http://www.mozilla.org/products/

Disable JavaScript in Thunderbird and Mozilla Suite.
Source: http://www.frsirt.com/english/advisories/2006/0413

36. *February 02, FrSIRT* — **Microsoft Windows SSDP and UPnP services privilege escalation issue.** A vulnerability has been identified in Microsoft Windows, which could be exploited by malicious users to obtain elevated privileges. This issue is due to an access validation error in the Simple Service Discovery Protocol (SSDP) and the Universal Plug and Play Device Host (UPnP) services that fail to properly validate user permissions, which could be exploited by local unprivileged attackers to bypass security restrictions and execute malicious programs with elevated privileges.
Solution: The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/0417

37. *February 02, Security Tracker* — **Netscape '−moz−binding' property validation flaw lets remote users conduct cross−domain scripting attacks.** A vulnerability was reported in Netscape. A remote user can conduct cross−domain scripting attacks. The Netscape browser '−moz−binding' CSS property does not properly restrict HTML code from other domains before displaying the input. A remote user can create specially crafted HTML that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code can originate from an arbitrary domain but will run in the security context of the domain serving the HTML. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the domain, access data recently submitted by the target user via Web form to the domain, or take actions on the domain acting as the target user.
Solution: No solution was available at the time of this entry.
Source: http://www.securitytracker.com/alerts/2006/Feb/1015563.html

38. *February 02, Websense Security Labs* — **Trojan Horse/WMF exploit: Fake bird flu epidemic e−mail.** Websense Security Labs has received reports of a Trojan horse that attempts to trick users into visiting a malicious Website to run malicious code. Users receive an e−mail with the subject, "Attention Bird Flu in England." The body requests users to click on a link to go either of two Websites to get more information. The e−mail also claims the government is trying to hide the facts on the flu. Upon clicking on a link, users are directed to a Website which claims that you have been blocked from accessing it. This appears to be another trick by the attacker to make the user believe that the site has either been disabled or shutdown. However, within the HTML, an IFRAME is loaded that uses the recent WMF exploit to run code without user−intervention. The code is a Trojan horse downloader, which connects to another site to download new malicious code. The filename is "expl1.wmf," which downloads and runs "expl1.exe." In the past, the same sites have been used for phishing, fraud, and distributing malicious code. The sites are hosted in the .WS and .CC domains and were up and running at the time of this alert.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =415

39. *February 01, Security Focus* — **Symantec Sygate Management server SMS authentication servlet SQL injection vulnerability.** Symantec Sygate Management Server is prone to an SQL injection vulnerability. The vulnerability specifically affects the SMS Authentication Servlet component of the server. A remote attacker can pass malicious input to database queries

through HTTP GET requests, resulting in modification of query logic or other attacks. This allows attackers to overwrite the password of any account on the server. This can facilitate a complete compromise if the attacker can overwrite the administrator password.
Solution: Symantec has released SYM06−002 to address this issue.
Source: http://www.securityfocus.com/bid/16452/references

40. *February 01, Register (United Kingdom)* — **UK tycoon charged with computer hacking.** Matthew Mellon, the heir to a $11.7 billion oil and banking fortune, has been charged with a computer hacking offense over his alleged involvement in a snooping, bugging and blackmail ring in the United Kingdom. Mellon will appear alongside 17 other defendants in court later this month. Members of the group were arrested after a year long investigation by the Met Police into a detective agency run by a former policeman. Scotland Yard's probe unearthed evidence that suspects also broke into the National Health Service computers and stole medical files in order to facilitate blackmail. Investigators said members of the group donned false uniforms in order to gain access to premises where they left bugs. Mellon, chief designer at upmarket shoe firm Harry's, a company he created five years ago, is charged with conspiracy to cause unauthorized modification of computers. Another wealthy entrepreneur, Adrian Kirby, who made an estimated fortune of $115 million chiefly by running a waste disposal unit business, faces phone tapping, computer hacking and conspiracy to pervert the course of justice charges. Scott Gelsthorpe of Kettering, Northamptonshire, a former policeman in Essex, faces 15 charges. All 18 suspects face an appearance in court on Thursday, February 23.
Source: http://www.theregister.co.uk/2006/02/01/tycoon_hacking_charg e/

41. *February 01, Computer World* — **Conviction second−ever for transmission of obscene e−mail messages.** A California man accused of managing the computer system to send hundreds of thousands of pornography−related e−mail messages has pleaded guilty to violating a U.S. antispam law. Kirk F. Rogers of Manhattan Beach, CA, pleaded guilty in U.S. federal court in Arizona Tuesday, January 31, to violating the U.S. CAN−SPAM Act, according to the U.S. Department of Justice (DOJ). Rogers' plea is the second−ever U.S. conviction related to the transmission of obscene e−mail messages, the DOJ said. Rogers agreed to forfeit money obtained in his spamming operation and faces a maximum sentence of five years in prison for a one−count violation of CAN−SPAM (Controlling the Assault of Non−Solicited Pornography and Marketing Act). Sentencing is scheduled for June 5.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,108267,00.html?SKC=security−108267

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT continues to contact and receive reports from federal agencies that have been affected by the CME−24 virus.

The CME−24 worm actively disables anti−virus software on a host system and will also overwrite users' data files on the third of every month. This virus affects all recent versions of Microsoft Windows.

The CME−24 worm spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3, .ppt, .pps, .zip, rar, .pdf, .psd, and .dmp.

Agencies that observe communication from internal machines to the 207.172.16.155 address should investigate further to determine if these machines are infected. Several agencies have reported that the systems that were impacted had anti−virus but were not running the latest signatures.

US−CERT recommends the following course of action:

Ensure that the latest anti−virus definitions are loaded on servers and workstations.

Leverage Internet Content Filtering Solutions to block executable and unknown file types at the email gateway

Setting up an access control list to detect users from browsing to the aforementioned websites/IP addresses. LURHQ provides snort signatures related to the CME−24 worm on their website.

Monitoring of outbound traffic to identify potential malicious traffic or information leaks.

The infected host will also access a website with a web counter. This web counter shows how many machines have been infected, although it is expected that an infected machine may access the website on multiple occasions, thus inflating the number. The original web counter showed consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. However, recent web log postings suggest that the number is much closer to 300,000 unique addresses. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

Please report any validated agency connection to the 207.172.16.155 website during the last 30 days to the US−CERT for further correlation and analysis.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4556 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 4142 (oidocsvc), 113 (auth), 135 (epmap), 139 (netbios−ssn), 32768 (HackersParadise) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

42. *February 04, Associated Press* — **Five Alabama churches burn.** A series of fires erupted in isolated churches along rural back roads south of Birmingham, AL, early Friday, February 3, destroying or damaging five houses of worship in what authorities called an arson case with no discernible motive. Congregants alerted to the flames on a foggy night found some of the church buildings fully ablaze or collapsing into smoldering ruin. At one church, whose congregation dates back more than a century, members arrived just in time to put out a blaze that had been started under an American flag at the front of the sanctuary. The cluster of fires in Bibb County, about 25 miles southeast of Birmingham, were set by someone "as fast as they could drive from one location to the next," Chief Deputy Sheriff Kenneth Weems said. Jim Cavanaugh, head of the federal Bureau of Alcohol, Tobacco, Firearms and Explosives office for Alabama and Tennessee, said it was clear that the fires were purposely set. Unlike in a 1996 outbreak of fires at black churches in Alabama and elsewhere, there was no common thread of race in this case. Four of the churches have white congregations, and one congregation is black. All were Baptist, the dominant faith in the area.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/02/03/AR2006020301451.html

[Return to top]

General Sector

43. *February 03, San Antonio News (TX)* — **IED's among weapons seized in Laredo raids.** Improvised explosive devices (IED), the home made bombs which have killed and maimed so many U.S. troops in Iraq, were among the items seized in three raids in the Texas border city of Laredo, federal officials said on Friday, February 3. Julie Myers, the Assistant Secretary of the Department of Homeland Security, said that the raids at three homes in Laredo, on January 12, January 27, and February 2, seized stacks of automatic weapons, grenades, gunpowder, ammunition, and drugs, as well as IEDs. She said a total of six people have been arrested in the three raids, and the investigations are continuing. "This is the first instance that we're aware of that we have found the IEDs," she said. "It is disconcerting to us to see the trends from assault weapons to IEDs." Myers said it appears to be an increase in weaponry used in the bloody year−long war between the Gulf Cartel and the Federation, two Mexican gangs fighting for control of what's called "The Plaza," the lucrative drug and immigrant smuggling routes into the

southwestern United States.
Source: http://www.woai.com/news/local/story.aspx?content_id=B657E5EE−5DA2−4D1D−A631−BEE02ECE9F59

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer